PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-143738
(43)Date of publication of application : 28.05.1999

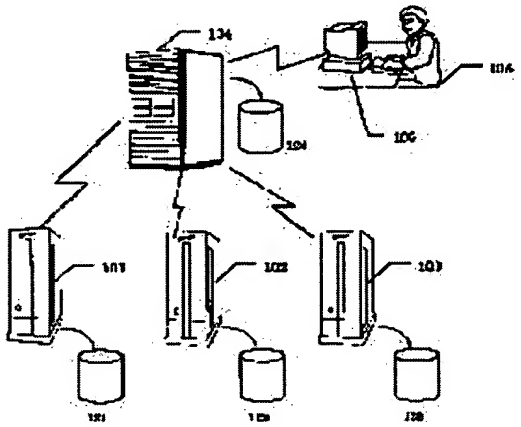
(51)Int.Cl. G06F 11/30
G06F 13/00

(21)Application number : 09-306068
(22)Date of filing : 07.11.1997

(71)Applicant : HITACHI LTD
(72)Inventor : URANO AKIHIRO
HIRATA TOSHIAKI
FUJINO SHUJI
SATO TOSHIO

(54) SUPERVISORY METHOD OF COMPUTER SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To collect the amount of logs which is necessary and sufficient to grasp an agent state without imposing processing load that is more than required upon a network and a manager computer by providing a means which simultaneously supervises logs collected from plural computers, checks a faithless deed and log contradiction by comparing them and detects them.
SOLUTION: Computers 101 to 103 respectively output logs and all of them are stored in auxiliary storage devices 121 to 123 respectively. Also, information what logs are collected is stored in an auxiliary storage device 124, is transferred to the computers 101 to 103 whenever necessary and is stored in the devices 121 to 123. Summaries of the logs which are stored in the devices 121 to 123 and logs that are thought as important are sent to a computer 104 through a network. The computer 104 individually analyzes the transferred logs, simultaneously supervises them and checks events that can be found.



LEGAL STATUS

[Date of request for examination]	31.08.2000
[Date of sending the examiner's decision of rejection]	14.05.2002
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3351318
[Date of registration]	20.09.2002
[Number of appeal against examiner's decision	2002-10472

of rejection]

[Date of requesting appeal against examiner's decision of rejection] 12.06.2002

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－143738

(43)公開日　平成11年(1999)５月28日

(51)Int.Cl.[6]	識別記号	ＦＩ		
G06F 11/30		G06F 11/30		E
13/00	351	13/00	351	N

審査請求　未請求　請求項の数６　ＯＬ　（全９頁）

(21)出願番号　特願平9－306068

(22)出願日　平成９年(1997)11月７日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　浦野　明裕
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　平田　俊明
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　藤野　修司
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内

(74)代理人　弁理士　小川　勝男

最終頁に続く

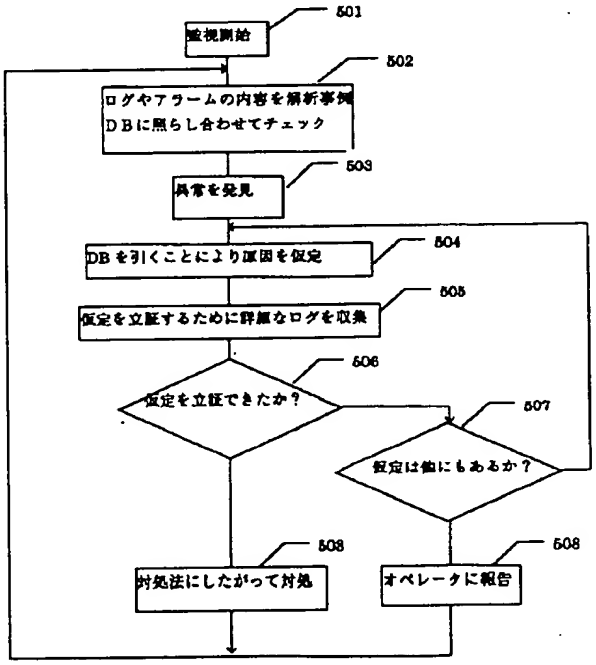
(54)【発明の名称】計算機システムの監視方法

(57)【要約】

【課題】本発明はネットワーク、マネージャ計算機に必要以上の処理負荷をかけることなく、必要十分な量のログを収集し、さらに詳細な情報を得るという作業を自動化する。さらに、異常箇所の特定と程度をわかりやすく表示すること。

【解決手段】アラームまたはログを監視する計算機が監視される側の監視レベルを設定する手段と、複数の計算機から収集されたログを同時に監視し、それらを合わせて見ることによって発見できる不信な行為や、それらのログの矛盾をチェックすることによって不信な行為を検出する手段と、ログの出力内容から、原因に関して仮説を立て、それを立証するために詳細なログを収集し、要因を絞り込む手段と、不信な計算機を表示する表示手段を提供する。さらに、ログに電子署名を行う手段と、ログの一部が紛失または改ざんされた場合に復元する手段を提供する。

図5



1

【特許請求の範囲】
【請求項１】複数の計算機と管理マネージャ計算機とがネットワークに接続された計算機システムに用いる計算機システムの監視方法であって、
複数の計算機から収集されたログを同時に監視し、それらをつき合わせて見ることによって発見できる不信な行為や、それらのログの矛盾をチェックすることによって不信な行為を検出する手段を有することを特徴とする計算機システムの監視方法。
【請求項２】請求項１に記載の計算機システムの監視方法において、
各計算機は、アラームまたはログを出力する手段を有し、
管理マネージャ計算機が管理対象とする計算機の監視レベルを設定する手段を有することを特徴とする計算機システムの監視方法。
【請求項３】請求項１に記載の計算機システムの監視方法において、
ログに出力された内容から、その原因に関して仮説を立て、それを立証するためにさらに詳細なログを収集し、原因を絞り込む手段を有することを特徴とする計算機システムの監視方法。
【請求項４】請求項１に記載の計算機システムの監視方法において、
不信な挙動を示す計算機のあやしさの度合いや、あやしい計算機が存在する可能性がある範囲に応じて監視画面上の色を変化させる手段と、警告音を変化させる手段を有することを特徴とする計算機システムの監視方法。
【請求項５】請求項１に記載の計算機システムの監視方法において、
ログを保存または転送する前に電子署名を行う手段と、ログに冗長なデータを付加することにより、ログの一部が紛失または改ざんされた場合においても元のログデータを復元できる手段とを有することを特徴とする計算機システムの監視方法。
【請求項６】請求項１または５に記載の計算機システムの監視方法において、
ログを複数の計算機に分割して保存しておくことにより、分割されたログの一部が紛失または改ざんされた場合においても元のデータを復元でき手段を有することを特徴とした計算機システムの監視方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、計算機の運用管理に関し、特に計算機のログの取り扱いの技術に関する。
【０００２】
【従来の技術】従来、コンピュータの各種ログをネットワークを利用して転送し、別のコンピュータにおいて監視することは広く行われてきた。それらはログを全て転送してしまうものがほとんどであった。しかし、全てのログを転送することはネットワークの負荷を増加させることになり、特にネットワークの転送能力に比較して出力されるログの量が多い場合に問題になる。また、ログを収集した計算機にとっても大量の収集されたログをすべて解析するのは解析処理に負荷がかかり、やはり問題になっている。そのため、オペレーティングシステムのなかには、ログのメッセージごとに重要度を付加し、その重要度に応じて破棄するのか、ログファイルに記録するのか、別の計算機に転送するのかなどの判別を行うものがある。このように、従来、ログを転送する際に重要と思われるログのみを抽出し、転送することが考えられているが、重要なログであるかどうかはログを出力した側の計算機の基準にしたがって判断しており、本当にネットワークの負荷や収集した計算機の負荷を軽くしているかどうかは一概には言えなかった。また、重要であるかどうかの基準をログを出力した側の計算機の基準で決めているため、監視を行う計算機においては重要な情報がログを抽出する計算機では重要でない情報と判断され転送されないことがあるなどの問題があった。

2

【０００３】また、上記従来例では、複数の計算機から出力されたログの関連付けや出力されたログに基づきさらに詳細な情報を得るという作業は管理者の判断で手作業で行う必要があった。
【０００４】さらに、例えば、「ＴＣＰ／ＩＰとＯＳＩネットワーク管理、ＳＲＣ」に記載のように、出力される情報の重要度に応じて画面上の色を変化させることは行われているが、それはそのホストの情報の重要度のみに応じて変化させているだけであった。
【０００５】従来、コンピュータのログ記録方式としては、ログ情報をそのまま補助記憶装置に書き出す方式が知られていた。補助記憶装置はローカルな補助記憶装置を用いることが普通であるが、ネットワークを用いリモートな補助記憶装置に記録することも行われていた。
【０００６】しかし、これらは動作記録をそのままの状態で補助記憶装置に書き出しており、動作記録が出力されてから補助記憶装置に保存されるまでの通信中やコンピュータ内部において、あるいは主記憶装置や補助記憶装置に記録されている間に、情報が変化あるいは改ざんされたとしても、それを検出することはできず、よって、保存されているログを読み取ったときにその正当性を検査することはできなかった。また、何らかの手段を用いてログ情報が変化あるいは改ざんされていることがわかった場合、もとのログを復元することはできなかった。
【０００７】
【発明が解決しようとする課題】本発明はネットワークに必要以上の負荷をかけることなく、さらにマネージャ計算機に必要以上の処理負荷をかけることなく、さらに、エージェントの状態の把握に必要十分な量のログを収集する方法及びプログラム、さらにはそれを用いた計

算機又はシステムを提供するものである。

【０００８】さらに、本発明は一個所の計算機の状態を監視するだけではわからない事象を検出する方法及びプログラム、さらにはそれを用いた計算機又はシステムを提供するものである。

【０００９】さらに、本発明は計算機に異常が発生した場合に、オペレータが監視画面を見た瞬間にどの計算機のどのあたりがどの程度異常になっているかをわかりやすく表現する方法及びプログラム、さらにはそれを用いた計算機又はシステムを提供するものである。

【００１０】さらに、本発明は複数の計算機から出力されたログの関連付けや出力されたログに基づきさらに詳細な情報を得るという作業を自動化することで管理者の負担を軽減させる方法及びプログラム、さらにはそれを用いた計算機又はシステムを提供するものである。

【００１１】さらに、本発明は計算機から出力されるログが途中で改ざんされたり、盗聴されたり、偽のログを紛れ込ませたりするのを防ぎ、さらに、一部を改ざんされた場合にでも元の情報を復元できる方法及びプログラム、さらにはそれを用いた計算機又はシステムを提供するものである。

【００１２】

【課題を解決するための手段】本発明の計算機監視方式は複数の計算機から収集されたログを同時に監視し、それらを合わせて見ることによって発見できる不信な行為や、それらのログの矛盾をチェックすることによって不信な行為を検出する。

【００１３】本発明の計算機監視方式はアラームまたはログを監視する計算機が監視される側の監視レベルを設定する。

【００１４】さらに、本発明の計算機監視方式はログに出力された内容から、その原因に関して仮説を立て、それを立証するためにさらに詳細なログを収集し、原因を絞り込む。

【００１５】さらに、本発明の計算機監視方式は不信な挙動を示す計算機のあやしさの度合いや、あやしい計算機が存在する可能性がある範囲に応じて監視画面上の色を変化させたり、警告音を変化させたりする。

【００１６】さらに、本発明の計算機監視方式はログを保存したり、転送する前に電子署名を行う。

【００１７】さらに、本発明の計算機監視方式はログに冗長なデータを付加することにより、ログの一部が紛失または改ざんされた場合においても元のログデータを復元できる。

【００１８】さらにまた、本発明の計算機監視方式はログを複数の計算機に分割して保存しておくことにより、分割されたログの一部が紛失または改ざんされた場合においても元のデータを復元できる。

【００１９】

【発明の実施の形態】ログを出力し、監視される側の計

算機をエージェントと呼び、ログを解析することによりエージェントを監視する側の計算機をマネージャと呼ぶ。また、文章および図の中においてデータベースをＤＢと略して書くことがある。

【００２０】図１において、計算機１０１、１０２および１０３は監視対象の計算機、計算機１０４は監視作業を行う計算機である。計算機１０１、１０２および１０３はそれぞれログ１１１、１１２および１１３を出力し、それらは全てそれぞれ補助記憶装置１２１、１２２および１２３に格納される。また、どのようなログを収集するのかという情報は補助記憶装置１２４に格納されており、必要に応じて計算機１０１、１０２、１０３に転送され、補助記憶装置１２１、１２２、１２３に記憶される。なお、この図ではエージェントは１０１、１０２、１０３の３台のみが記述されているが、３台に限定される必要はない。また、マネージャである計算機１０４とエージェントが同一の個体である形体を取ってもよい。

【００２１】また、図２は図１のエージェントとマネージャを１台ずつ抜き出し、詳細を書いた図である。あらかじめ補助記憶装置である解析ルール事例データベース２０１には図４に示されるようなログから得られた事象に対する仮定すべき原因、それを立証するためにどのような調査を行えばよいか、また、立証されたときにどのような処置を行えばよいかが記録されている。データ解析部２０３はあらかじめ収集項目制御部２０４を通して、解析ルール事例の一部をエージェントに転送しておく。転送された解析ルールは補助記憶装置２２１に記憶される。

【００２２】アプリケーションプログラム２２４から出力されたログは補助記憶装置であるログデータベース２２３に記憶される。

【００２３】図３に計算機101, 102, 103, 104, 106のハードウエア構成を示す。

【００２４】図３に示すように各計算機は、中央処理装置（３０２）と、主記憶装置（３０１）と、通信回線（３０５）やローカルエリアネットワーク（３０４）等のネットワークとの間のデータの入出力を制御するネットワーク制御装置（３０３）と、デイスク装置（３０６）およびその入出力を制御するデイスク制御装置（３０７）と、表示装置（３０８）およびその入出力を制御する表示制御装置（３０９）とを備えて構成されている。

【００２５】図４に解析ルール事例データベースの一例を示す。データベースは表形式になっており、ログから得られて情報、考えられる原因、仮定を立証するために必要な調査方法、および立証されたときの対処方法が記憶されている。

【００２６】また、図５にデータ解析部２０３が収集されたログデータを解析する手順をフローチャートによっ

て示す。

【００２７】エージェント２２５のログフィルタ２２２は解析事例データベース２２１に従ってログデータベース２２３からデータを取り出し、マネージャ２０７のログ収集部２０５へ転送する。転送されたデータはログデータベース２０６に保存される。データ解析部２０３は解析ルール事例データベース２０１に従って、ログ収集部２０５からログデータを得、データを解析する。このとき必要に応じて収集項目制御部２０４にさらに詳細なログの収集を指示する。また、収集項目制御部２０４はマシンの負荷の状況やネットワークの負荷および収集されてきているログの量などを解析ルール事例データベースに照らし合わせて、収集するログの項目を制御する。

【００２８】また、データ解析部２０３における解析結果はコンソール制御部２０２に送られ、さらにコンソール計算機の中にあるコンソール制御部２１２に送られ、画面表示２１１に表示される。

【００２９】オペレータからの指示はキーボード入力２１３およびマウス入力２１５から行われ、コンソール制御部２１２およびコンソール制御部２０２を通り、データ解析部２０３に送られる。

【００３０】再び図１を用いて説明を行う。補助記憶装置121, 122, 123に記憶されたログの要約や重要だと思われるログはネットワークを経由して計算機１０４に送られる。

【００３１】何に関するログが重要で計算機１０４に送らなくてはいけないかというルールはあらかじめ計算機１０４から計算機１０１、１０２、１０３に指示しておく。この指示はシステムを構築したときに行われるほか、計算機１０４が必要と判断するたびに行われる。例えば、ネットワークの負荷が高くなっている時や計算機１０４の負荷が高くなっている時などは本当に重要なログだけを転送することにより転送するログの量を少なくなるよう指示したり、監視を強めたいときはあまり重要でないと思われるログも転送するように指示をしたりする。

【００３２】計算機１０４は転送されたログ１３１、１３２および１３３を個別に解析し、監視するほか、それらを同時に監視し、それらをあわせて見ることによって発見できる事象をチェックする。

【００３３】またオペレータ１０５はコンソール計算機１０６を操作する。コンソール計算機１０６は計算機１０４に対し、必要な情報を提供するよう要求し、計算機１０４は要求された情報が自分の補助記憶装置１２４に記録されていればそれを返答する。リモートにある計算機１０１、１０２、１０３に問い合わせないとわからない情報が要求された場合、コンソール計算機にリモート計算機に問い合わせる必要があることを通知し、リモート計算機に問い合わせるかどうかオペレータの指示を待つ。オペレータが取り寄せる旨、指示した場合、計算機１０４は計算機１０１、１０２、１０３と通信を行い、ログを取り寄せ、その結果をコンソール計算機１０６に通知する。

【００３４】この例では、計算機１０４が答えられない場合、オペレータ１０５に問い合わせる間、指示を待っているが、先行して計算機１０１、１０２、１０３と通信を行い、情報を取り寄せておくことにより、オペレータ１０５が取り寄せる指示を出してから計算機１０４が返答できるまでの時間を短縮することができる。

【００３５】また、この例では計算機１０４が答えられない場合、オペレータ１０５にリモートの計算機に問い合わせるべきかどうかの判断を委ねたが、この判断は計算機１０４またはコンソール計算機１０６が行う構成も考えられる。

【００３６】また、この例ではより詳しい情報を収集する最初のきっかけをオペレータ１０５が行っているが、これはコンソール計算機１０６、計算機１０４がそれまでに収集されているログをチェックすることにより自動的に判断する構成も考えられるし、計算機１０１、１０２、１０３のうちいづれかが自ら判断し、情報の収集の必要性をアラームという形で計算機１０４に通知する構成も考えられる。

【００３７】さらに、計算機１０４は自分の保持する情報のみでは要求に答えられないと判断した時、やみくもに計算機１０１、１０２、１０３に情報を要求するのではなく、計算機１０１、１０２、１０３において何が起こっているのかを仮定し、それを証明するために計算機１０１、１０２、１０３に問い合わせる構成が考えられる。例えば、計算機１０１と１０２は通信を行いながら計算処理を行っているとする。計算機１０１で補助記憶装置があふれたり、機器の故障が起こったりなどして計算機１０２と正常な通信が行えなかったとする。計算機１０２はその通信が正常に行えなかったことを検知できずに処理を続け、誤った答を出力する。計算機１０４、コンソール計算機１０６、オペレータ１０５のいづれかがその異常な答えに気づいた場合、計算機１０４はさらなる情報の収集を行うことになるが、この時、「計算機１０２が異常な答えを出力したのは計算機１０１との通信が正常に行われなかったからではないか」と仮定し、計算機１０１か１０２のいづれかもしくは両方に通信の記録を提出するよう要求する。その記録から通信が正常に行われていないことが判明すればそこが原因であったことが証明されたことになる。さらに、その通信の異常は計算機１０１の補助記憶装置があふれたことが原因であると仮定し、計算機１０１に補助記憶装置に関する情報を報告させる。補助記憶装置があふれているという報告があった場合、計算機１０４の仮定が正しかったことが証明される。

【００３８】以上の仮定を図６においてフローチャートにて示す。

【００３９】この例においては、原因となる事象を仮定し、それを検証するためにログを収集するという過程を経ることにより、最初の段階では計算機１０１や１０２のログのうち一部のみを転送すればよいことや、仮定を検証するために詳細なログを収集するときにでも仮定を検証するために必要なログのみを収集するために収集するログの量を少なく押さえることができ、そのため計算機１０４の解析負荷を低く押さえたり、ネットワークのトラフィックを低く押さえることができるといった効果が期待される。

【００４０】また、これまでの例においてはリアルタイムに処理する様子を記述したが、計算機１０４がログを収集するタイミングは一定期間ごとにおこなってもよく、その場合はバッチ的に処理することにより同様の処理が可能である。

【００４１】図９は、コンソール計算機１０６において、オペレータ１０５に情報を提示する時に重要度や異常な範囲によって色を変化させるようすをあらわした画面（９０１）である。例えば、上記例において、計算機１０２から異常な答が出力されたことを検出した場合、計算機１０１と１０２の通信が異常であったと仮定した段階でコンソール計算機１０６の画面上において計算機１０１と１０２を示す部分が黄色の警告表示で囲むように表示される（９０１）。さらに計算機１０１が原因と仮定された段階で表示９０２の代わりに計算機１０１の表示を赤く表示する（９０３）。この例では仮定された段階で色を変化させたが、証明された段階において色を変化させることとするのもよい。

【００４２】また、ここまで計算機１０４は計算機１０１、１０２、１０３に関する全般的な事柄を監視するものとしてきたが、特にコンピュータセキュリティに特化した監視システムも考えられる。

【００４３】例えば、計算機１０４がログに示された情報からその原因を仮定し、それを証明するためにより詳細な情報を収集するシステムにおいて、以下のようなものが考えられる。図７を用いて説明する。

【００４４】コンピュータネットワークにおける侵入者がデータを盗み出す場合、必要なデータのみを盗み出すのではなく、読み取ることのできるデータを全て侵入者の手元のコンピュータに転送し、あとからそれらを解析する方法が取られることがある。そのような場合、ネットワークにおけるファイル転送量が通常を大きく上回る。そこでネットワーク上におけるファイルの転送量を監視しておき、通常のトラフィックを大きく上回るファイル転送量を検出した場合（７０２）、データベースから自動バックアップを行っているのではないかと仮定する（７０３）。

【００４５】そこで、その仮定を立証するために、自動バックアップのスケジュールおよび実行状況を調査する（７０４）。ファイル転送を行っている計算機が自動バックアップの対象になっていないこと、あるいはスケジュールが組まれていないことを発見すると「自動バックアップを行っている」という仮定は却下される（７０５）。

【００４６】さらに解析ルール事例データベース２０１を参照することにより、管理者が手動でバックアップを行っていると仮定する（７０６）。その仮定を立証するためファイル転送を行っている者がバックアップを行う権限を持っているか、およびバックアップを行う命令を発行したかどうかを調査する（７０７）。

【００４７】その結果、ファイル転送を行っている者はバックアップの権限を持っていないことを発見すると「手動バックアップを行っている」という仮定は却下される（７０８）

さらにデータベースを検索すると「侵入者がデータを持ち出している」と仮定できる（７０９）。そこでファイル転送を行っている者の使用計算機、ファイル転送先をチェックする（７１０）。その結果、侵入者がデータを不正に持ち出していることを発見し（７１２）、仮定が立証される（７１２）。

【００４８】さらに以下、図１０を用いてログ改ざん防止に関する発明の説明を行う。

【００４９】計算機1001はプログラムの実行結果などをログとして出力する。この出力されたログに付加情報を持たせながら分割し、さらに電子署名を行った後、暗号化する。ここで付加情報というのはログがn個に分割された場合、n個未満の個数のログを見るだけで、元の情報が取り出せるように工夫した情報のことである。例えば元のログに付加情報を加えてa, b, cの３つのログに分割した場合、いづれか２つを読み出すことにより元の情報を取り出せるよう工夫した情報である。

【００５０】具体的な一例をあげると、出力されたログが１行１０２４文字のログを３台の計算機で分割して記憶する場合には、前半５１２文字と、後半５１２文字とに分割し、また前半部分と後半部分のXORを取ったものを付加情報とする。ここで前半部分と後半部分のXORというのは前半部分の１文字目と後半部分の１文字目のXORをとったものを１文字目とし、以下２文字目、３文字目と５１２文字目まで同様に繰り返して生成された文字列のことをいう。

【００５１】ログは通信線1002, 1003, 1004を通り、それぞれ計算機1005, 1006, 1007が受け取る。計算機1005, 1006, 1007は受け取ったログ情報を復号化したのち、記憶装置に保存する。

【００５２】計算機1011はログを読み出すにあたって、通常計算機1005, 1006, 1007の３台にアクセスすることにより計算機1001が出力したログを読み出すことができるが、計算機1005, 1006, 1007のうちいづれかの１台の記憶装置の内容が変化、改ざんされていた場合でも、他の２台の情報から計算機1001が出力したログを復元すること

ができる。

【００５３】さきほどのXORの例でいえば前半５１２文字のデータ、あるいは後半５１２文字のデータが失われてしまったとしても、前半後半のデータのうち、失われていない方のデータとXORしたデータとのＸＯＲを計算することにより、失われてしまったデータを復元することができる。

【００５４】ここでは計算機1001において、ログに付加情報を加え分割した後、認証情報を加え暗号化を行っているが、認証情報を加える作業と付加情報を加え分割する作業と、暗号化は、そのいづれかもしくは全部を行わないことも可能である。その場合は計算機1011において、それらに対応した処理を省くこととする。

【００５５】また、ここではログを出力する計算機と記憶する計算機と読み出す計算機を別の個体としたが、これらは一つの個体の内部において実現されてもよい。

【００５６】以上に説明したように、本発明によれば、ネットワークおよびマネージャ計算機に必要以上の処理負荷をかけることなく、さらに、エージェントの状態の把握に必要十分な量のログを収集することが可能となる。

【００５７】さらに、本発明によれば、一個所の計算機の状態を監視するだけではわからない事象を検出することが可能となる。

【００５８】さらに、本発明によれば、計算機に異常が発生した場合に、オペレータが監視画面を見た瞬間にどの計算機システムの異常の範囲と異常の程度が容易に把握できる。

【００５９】さらに、本発明によれば複数の計算機から出力されたログの関連付けや出力されたログに基づきさらに詳細な情報を得るという作業を自動化することで管理者の負担を軽減させることができる。

【００６０】さらに、本発明によれば計算機から出力されるログが途中で改ざんされたり、盗聴されたり、偽のログを紛れ込ませたりするのを防ぎ、さらに、一部を改ざんされた場合にでも元の情報を復元することができる。

【００６１】

【発明の効果】以上に説明したように、、本発明によれば、システムに発生する事象を正確に検出することが可能となり、異常が発生した場合でもその範囲と程度を容易に把握できる。また、データを復元することも可能になる。

【図面の簡単な説明】

【図１】本実施例に係る計算機システムの全体構成図。

【図２】マネージャが、各計算機のログを収集／解析することにより各計算機を監視するためのシステム構成を表す図。

【図３】マネージャおよびエージェントの各計算機のハードウエア構成図。

【図４】解析ルール事例ＤＢの内容の一例を表す図。

【図５】ログに出力された内容から、その原因に関して仮説を立て、それを立証するために詳細なログを収集し、要因を絞り込む基本手順を表す図。

【図６】ログに出力された内容から、その原因に関して仮説を立て、それを立証するためにさらに詳細なログを収集し、要因を絞り込む手順の一例。

【図７】ログに出力された内容から、その原因に関して仮説を立て、それを立証するためにさらに詳細なログを収集し、要因を絞り込む手順の一例。

【図８】ログに出力された内容から、その原因に関して仮説を立て、それを立証するためにさらに詳細なログを収集し、要因を絞り込む過程において、コンソールの画面上に色表示を行うことを含めた手順の一例。

【図９】オペレータの監視画面の一例を表す図。

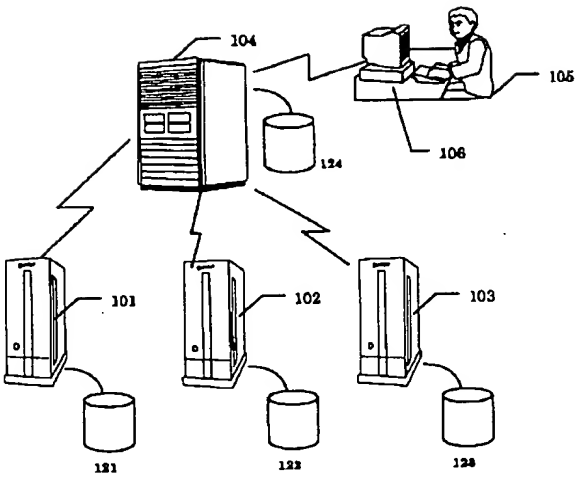
【図１０】ログの改ざん防止および改ざんされた場合の回復のためのシステム構成を表す図。

【符号の説明】

１０１～１０４：計算機、１０５：オペレータ、１０６：コンソール、１２１～１２４：補助記憶装置、２０１：解析ルール事例ＤＢ、２０２：コンソール制御部、２０３：データ解析部、２０４：収集項目制御部、２０５：ログ収集部、２０６：ログＤＢ、２０７：マネージャ、２１１：画面表示部、２１３：キーボード入力部、２１２：コンソール制御部、２２１：解析ルール事例ＤＢ、２２２：ログフィルタ、２２３：ログＤＢ、２２４：アプリケーションプログラム、２２５：エージェント、３００：計算機、３０１：主記憶装置、３０２：中央処理装置、３０３：ネットワーク制御装置、３０４：ローカルエリアネットワーク、３０５：通信回線、３０６：デイスク装置、３０７：デイスク制御装置、９０１：画面領域、９０２、９０３：障害の原因と推定される領域、１００１：ログ出力マシン、１００２～１００４、１００８～１０１０：ログデータ、１０１１：ログ表示マシン。

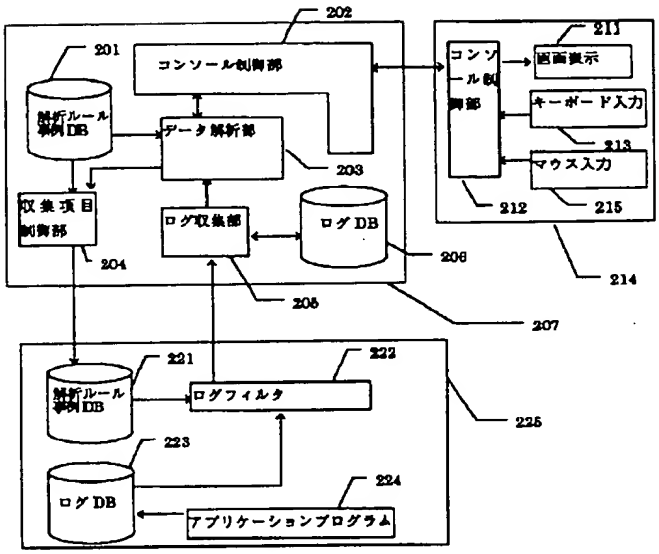
【図１】

図１



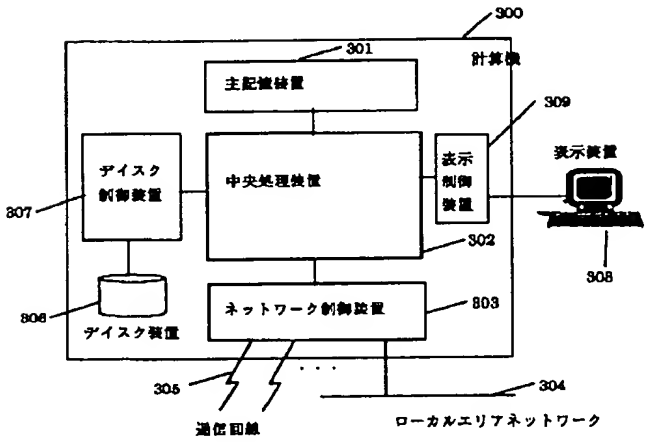
【図２】

図2



【図３】

図3



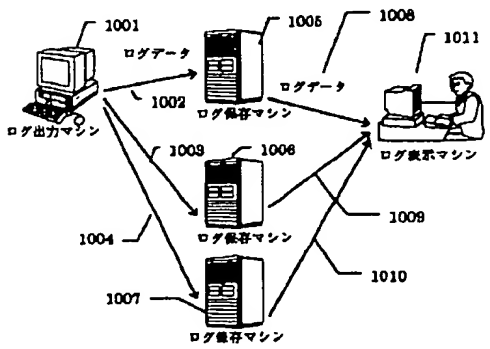
【図４】

図4

得られた情報	考えられる原因（仮定される原因）	調査方法	対処法
計算結果が合わない	通信が正常に行われていない	通信内容のログを検査	
通信が正常に行われていない	ディスクがあふれている	ディスクの空き容量をチェック	
ネットワークにおけるファイル転送量が異常に多い	自動バックアップを行っている	バックアップ計画・バックアップ装置の付いている計算機の状態を調査	バックアップを行っている場合は正常
同上	オペレータが手動でバックアップを行っている	ファイル転送を行っているユーザがバックアップを行う権限を持っているか、また、バックアップの命令を指示したかを調査	バックアップを行っている場合は正常
同上	侵入者がデータを盗み出している	データの転送を行っているユーザをチェック	オペレータに報告

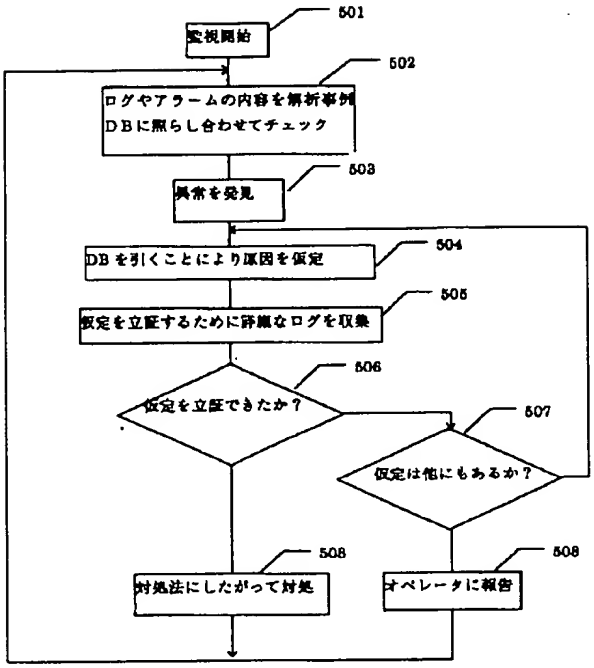
【図１０】

図１０



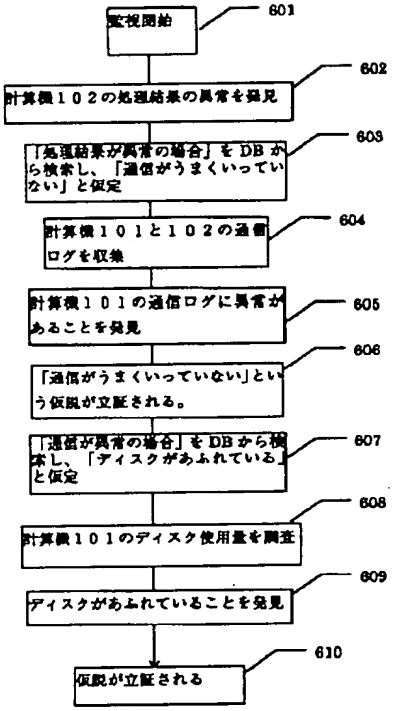
【図５】

図5



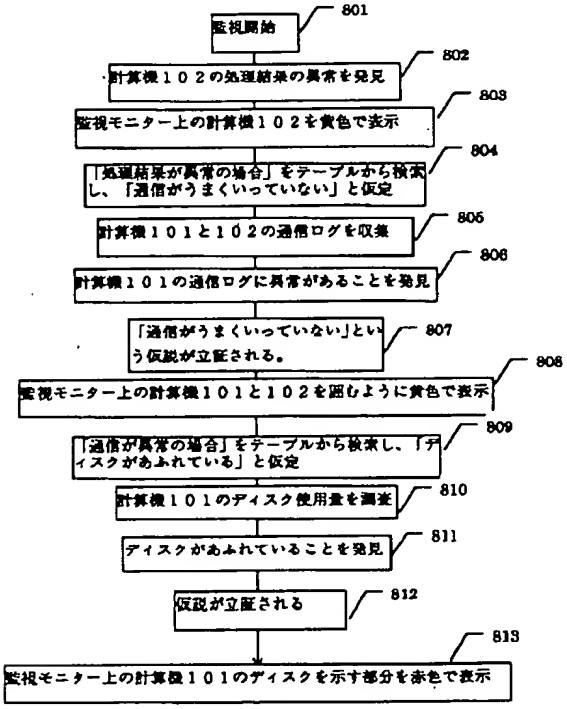
【図６】

図6



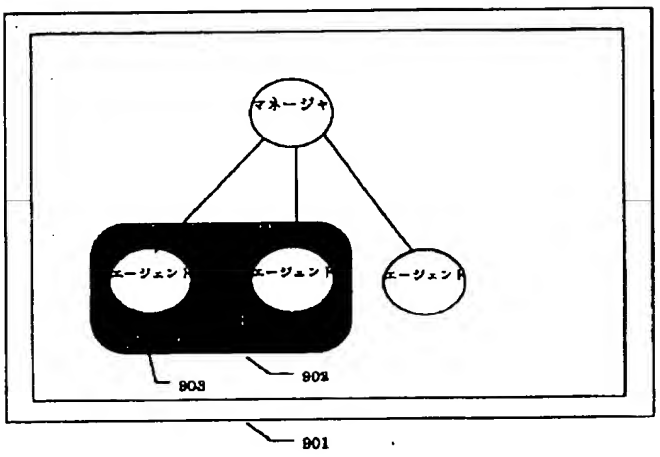
【図８】

図8



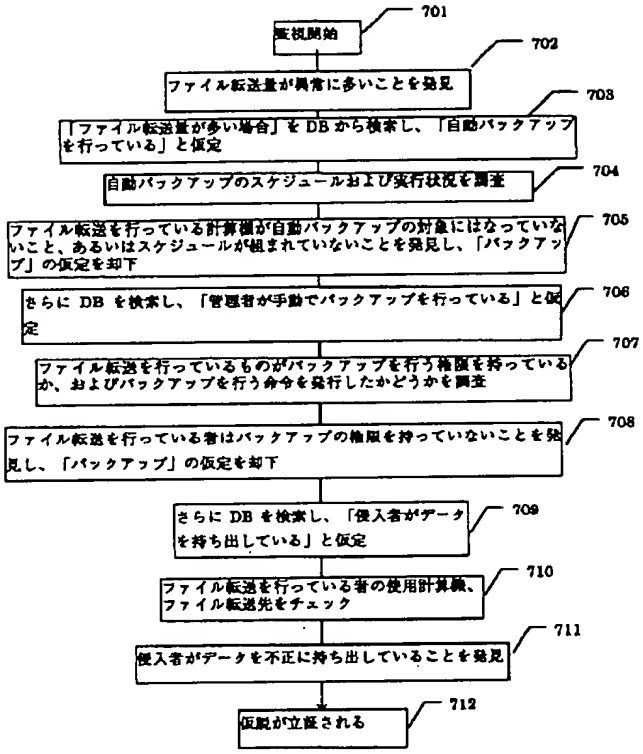
【図９】

図 9



【図７】

図7



フロントページの続き

(72)発明者　佐藤　敏夫
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内